Ln 19), where he discloses the generation of many graphs and correlating of each of them based on history and patterns.

The comments of the examiner do not address the features recited in Applicant's claim 7. Applicant's claim 7 recites producing a histogram of received network traffic for at least one parameter of network packets and characterizing an attack based on comparison of historical histograms with the produced histogram data for one or more parameters. These features are neither described nor suggested by Maloney. In order to support a rejection that a claim is anticipated by a reference, the examiner must show that a single reference describes each and every feature recited in the claim.

In addressing Applicant's prior response, the examiner contends that Maloney describes the features of claim 7 at col. 6, line 65 to col. 7, line 19. These passages are reproduced below:

Following parsing of the knowledge base 16 the analytical engine 20 responds to the data for preparation and converting into vector-based nodal diagrams. Typically the analytical engine 20 creates associations between a number of different charts to determine if such data charts correlate or differentiate. Relationships between an array of data sources is utilized to verify hypothesis, to correlate relationships among multiple data sets, and to identify target data within a large data set. Based on this analysis, the information security analysis system enables the development of resources for management of a network.

The analytical engine 20 analyzes network data to relate knowledge base data to session data, packet data, and alert data as these relationships are utilized to determine who has been talking to whom as well as the content of the traffic for specific protocols.

In the process of analyzing network data received by the discovery tool 12 (discovery engine) a determination must also be made as to what communication exist in more than one data set. Characterizing the data in this way utilizes taking a periodic snapshot of captured data over a time period. Averages are then made of what relationships exist to create a link chart representing traffic between data sets.

Maloney in these passages describes building vector-based nodal diagrams. However, Applicant has not claimed building vector based nodal diagrams. Rather, Applicant has claimed producing a histogram of received network traffic for at least one parameter of network packets. The nodal diagram, as taught by Maloney, is not built based on a least one parameter of network packets. In order for a reference to anticipate a claim the reference must disclose each and every element in the claim, as arranged in the claim. Maloney does not disclose the claimed feature of producing a histogram and fails to disclose producing a histogram of received traffic for at least one parameter of network packets.

Maloney fails to suggest must less disclose characterizing an attack based on comparison of a historical histogram with the produced histogram data for one or more parameters. Rather, Maloney seeks to analyze the data (session data, packet data and alert data) "to determine who has been talking to whom, as well as the content of the traffic." Maloney offers no guidance on how to use the vector-based nodal diagrams, much less a histogram, as claimed by Applicant, to characterize an attack and certainly fails to suggest comparing the produced histogram to an historical histogram of one or more parameters.

Maloney describes at Col. 10 line 37-45:

> **Data stored in a flat text file by operation of the discovery tool 12 is utilized by the KB summation tool of the knowledge base tool set 96 to create a statistical matrix of the data contained in packet and session logs. For example, the instance of a protocol may be used as the Y access and the source IP address may be used as the X access. After selection of the packet or session log has been made, the KB summation tool screens the appropriate log file and displays available access criteria to create a graph.**

Maloney describes "a statistical matrix of the data contained in packet and session logs. For example, the instance of a protocol may be used as the Y access and the source IP address may be used as the X access." Maloney fails to describe or suggest however, producing a histogram, and in particular fails to suggest producing a histogram for received network traffic for at least one parameter of network packets. The teaching of "the instance of a protocol may be used as the Y access and the source IP address may be used as the X access." does not describe a histogram.

Moreover, Maloney neither describes nor suggests characterizing an attack based on comparison of historical histograms with the produced histogram data for one or more parameters. Rather, at Col. 9, line 64 to Col. 7, line 6, Maloney describes the vector based nodal diagram:

> **Following parsing of the knowledge base 16 the analytical engine 20 responds to the data for preparation and converting into vector-based nodal diagrams. Typically the analytical engine 20 creates associations between a number of different charts to determine if such data charts correlate or differentiate. Relationships between an array of data sources is utilized to verify hypothesis, to correlate relationships among multiple data sets, and to identify target data within a large data set. Based on this analysis, the information security analysis system enables the development of resources for management of a network.**

Thus, Maloney seeks to provide the vector based nodal diagrams as a tool in analyzing data, namely, "to verify hypothesis, to correlate relationships among multiple data sets, and to identify target data within a large data set." No mention or guidance is given for characterizing an attack based on comparison of historical histograms with the produced histogram data for one or more parameters.

Thus, for these reasons and the reasons of record, claim 7 is neither described nor suggested by Maloney.

The examiner stated: "Regarding Claim 22, Maloney discloses the vector-based correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that can point to types of attacks and reduce dropping legitimate traffic see Col 6, Ln 63-Col 7 Ln 11." This excerpt from Maloney is reproduced below:

> **Following parsing of the knowledge base 16 the analytical engine 20 responds to the data for preparation and converting into vector-based nodal diagrams. Typically the analytical engine 20 creates associations between a number of different charts to determine if such data charts correlate or differentiate. Relationships between an array of data sources is utilized to verify hypothesis, to correlate relationships among multiple data sets, and to identify target data within a large data set. Based on this analysis, the information security analysis system enables the development of resources for management of a network.**
>
> **The analytical engine 20 analyzes network data to relate knowledge base data to session data, packet data, and alert data as these relationships are utilized to determine who has been talking to whom as well as the content of the traffic for specific protocols.**

Maloney, whether in the above passage or elsewhere, neither discloses nor suggests a process to correlate suspicious parameters to reduce blocking of legitimate traffic. Rather, Maloney discloses a technique to correlate relationships among multiple data sets in order to develop resources for management of a network.

The examiner rejected claims 1-6, 18-20, 22, and 28-37 under 35 U.S.C. 103(a), as being unpatentable over U.S. Patent 6,301,668 B1 Gleichauf et al. (hereinafter Gleichauf) in view of U.S. Patent 6,304,262 B1 to Maloney et al.(hereinafter Maloney).

In addressing Applicant's prior response, the examiner stated:

> **The Applicant's arguments regarding Claim 1 are not persuasive. As Maloney discloses the filtering of network traffic based on characterization process see Col 8 Ln 27-40. And the Gleichauf reference shows it monitoring device positioned between data center and network see Fig. 2 item 14. And further the**

thwarting of denial of service attacks based on a threshold see Col 8 Ln 58- Col 9 Ln 2. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case the combination of network traffic detection of Maloney and the use of threshold value to detect denial of service attacks.

Applicant's Claim 1 is not suggested by Gleichauf in combination with Maloney. Maloney does not discloses filtering of network traffic based on characterization process, as recited in claim 1. Rather, Maloney discloses (at Col. 8, Ln 27-40) a packet view tool and a filter that can be set up to capture updated packets. Maloney however fails to disclose the histogram, as discussed above, and thus fails to disclose filtering of network traffic based on characterization process. Gleichauf does not cure the deficiencies in Maloney.

Gleichauf does not show a monitoring device positioned between data center and network in Fig. 2 item 14, but more importantly fails to show: "a detection process to determine if the values of a parameter of network traffic exceed normal values for the parameter to indicate an attack on the data center." Apparently the examiner uses Gleichauf discussion of a threshold see Col 8, Ln 58-Col 9, Ln 2 to show this feature of Applicant's claim 1.

However, Gleichauf does not suggest to thwart a denial of service attack based on a threshold at Col 8, Ln 58 to Col 9, Ln 2. Rather, Gleichauf discloses processor utilization not a value of a parameter of network traffic.

Applicant contends that the examiner has not provided a proper motivation to support a the proposed combination of the references, for reasons of record. The examiner motivation from the prior action was that:

It would be obvious to one having ordinary skill in the art at the time of the invention to include the building of graph and the classifying of the attack in the invention of Gleichauf in order to allow the systems administrator to take appropriate measures as taught in Maloney see Col 7 Ln 40-Col 8 Ln 12. And further, Gleichauf discloses the possibly of visual representation see Fig. 3 item 64, thus the inclusion of a building a graph would be reasonable successful.

The examiner explains the motivation as: "In this case the combination of network traffic detection of Maloney and the use of threshold value to detect denial of service attacks." The

examiner still fails to explain why a person of ordinary skill would combine Gleichauf, which deals with vulnerability assessment, and Maloney, which deals with an information security analysis system. One would not be motivated by Gleichauf to look to an information security analysis system of Maloney to add the features of a histogram (which is absent in Maloney), since in claim 1 the histogram, as part of the characterization process, is used to detect a denial of service attack and is not merely used for "visual representation," as the examiner contends.

Applicant contends therefore that the combination of Gleichauf and Maloney fail to suggest claim 1. Applicant further contends that claims 2-6 add distinct limitations to claim 1 and that claims 18-20, which depend from claim 7 are allowable at least for the reasons discussed in claim 7. In addition, claim 22 is allowable with claim 21 and claims 28-37 are allowable for analogous reasons discussed in claim 7.

The examiner rejected Claim 25 under 35 U.S.C. 103(a) as being unpatentable over U.S. Maloney in view of Gleichauf.

The examiner stated in response to Applicant's prior response that: "As Maloney discloses the activation of filters (after installation) see Col 8 Ln 27-40."

Claim 25 is allowable over the references, since the references fail to suggest the features of the base claim 21, and fail to suggest that the device is a gateway device that is adaptable to dynamically install filters on nearby routers. While Maloney describes a packet filter, it is not shown that Maloney teaches to install the filter from a gateway onto nearby routers.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 2/7/06

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21236146.doc